IDENTITY THEFT PROTECTION ACT
Act 452 of 2004

AN ACT to prohibit certain acts and practices concerning identity theft; to require notification of a security breach of a database that contains certain personal information; to provide for the powers and duties of certain state and local governmental officers and entities; to prescribe penalties and provide remedies; and to repeal acts and parts of acts.

History: 2004, Act 452, Eff. Mar. 1, 2005;—Am. 2006, Act 566, Eff. July 2, 2007.

The People of the State of Michigan enact:

445.61 Short title.

Sec. 1. This act shall be known and may be cited as the "identity theft protection act".

History: 2004, Act 452, Eff. Mar. 1, 2005.

445.63 Definitions.

Sec. 3. As used in this act:

(a) "Agency" means a department, board, commission, office, agency, authority, or other unit of state government of this state. The term includes an institution of higher education of this state. The term does not include a circuit, probate, district, or municipal court.

(b) "Breach of the security of a database" or "security breach" means the unauthorized access and acquisition of data that compromises the security or confidentiality of personal information maintained by a person or agency as part of a database of personal information regarding multiple individuals. These terms do not include unauthorized access to data by an employee or other individual if the access meets all of the following:

(*i*) The employee or other individual acted in good faith in accessing the data.

(*ii*) The access was related to the activities of the agency or person.

(*iii*) The employee or other individual did not misuse any personal information or disclose any personal information to an unauthorized person.

(c) "Child or spousal support" means support for a child or spouse, paid or provided pursuant to state or federal law under a court order or judgment. Support includes, but is not limited to, any of the following:

(*i*) Expenses for day-to-day care.

(*ii*) Medical, dental, or other health care.

(*iii*) Child care expenses.

(*iv*) Educational expenses.

(*v*) Expenses in connection with pregnancy or confinement under the paternity act, 1956 PA 205, MCL 722.711 to 722.730.

(*vi*) Repayment of genetic testing expenses, under the paternity act, 1956 PA 205, MCL 722.711 to 722.730.

(*vii*) A surcharge as provided by section 3a of the support and parenting time enforcement act, 1982 PA 295, MCL 552.603a.

(d) "Credit card" means that term as defined in section 157m of the Michigan penal code, 1931 PA 328, MCL 750.157m.

(e) "Data" means computerized personal information.

(f) "Depository institution" means a state or nationally chartered bank or a state or federally chartered savings and loan association, savings bank, or credit union.

(g) "Encrypted" means transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key, or securing information by another method that renders the data elements unreadable or unusable.

(h) "Financial institution" means a depository institution, an affiliate of a depository institution, a licensee under the consumer financial services act, 1988 PA 161, MCL 487.2051 to 487.2072, 1984 PA 379, MCL 493.101 to 493.114, the motor vehicle sales finance act, 1950 (Ex Sess) PA 27, MCL 492.101 to 492.141, the secondary mortgage loan act, 1981 PA 125, MCL 493.51 to 493.81, the mortgage brokers, lenders, and servicers licensing act, 1987 PA 173, MCL 445.1651 to 445.1684, or the regulatory loan act, 1939 PA 21, MCL 493.1 to 493.24, a seller under the home improvement finance act, 1965 PA 332, MCL 445.1101 to 445.1431, or the retail installment sales act, 1966 PA 224, MCL 445.851 to 445.873, or a person subject to subtitle A of title V of the Gramm-Leach-Bliley act, 15 USC 6801 to 6809.

(i) "Financial transaction device" means that term as defined in section 157m of the Michigan penal code,

© Legislative Council, State of Michigan Courtesy of www.legislature.mi.gov

1931 PA 328, MCL 750.157m.

(j) "Identity theft" means engaging in an act or conduct prohibited in section 5(1).

(k) "Law enforcement agency" means that term as defined in section 2804 of the public health code, 1978 PA 368, MCL 333.2804.

(*l*) "Local registrar" means that term as defined in section 2804 of the public health code, 1978 PA 368, MCL 333.2804.

(m) "Medical records or information" includes, but is not limited to, medical and mental health histories, reports, summaries, diagnoses and prognoses, treatment and medication information, notes, entries, and x-rays and other imaging records.

(n) "Person" means an individual, partnership, corporation, limited liability company, association, or other legal entity.

(o) "Personal identifying information" means a name, number, or other information that is used for the purpose of identifying a specific person or providing access to a person's financial accounts, including, but not limited to, a person's name, address, telephone number, driver license or state personal identification card number, social security number, place of employment, employee identification number, employer or taxpayer identification number, government passport number, health insurance identification number, mother's maiden name, demand deposit account number, savings account number, financial transaction device account number or the person's account password, stock or other security certificate or account number, credit card number, vital record, or medical records or information.

(p) "Personal information" means the first name or first initial and last name linked to 1 or more of the following data elements of a resident of this state:

(*i*) Social security number.

(*ii*) Driver license number or state personal identification card number.

(*iii*) Demand deposit or other financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to any of the resident's financial accounts.

(q) "Public utility" means that term as defined in section 1 of 1972 PA 299, MCL 460.111.

(r) "Redact" means to alter or truncate data so that no more than 4 sequential digits of a driver license number, state personal identification card number, or account number, or no more than 5 sequential digits of a social security number, are accessible as part of personal information.

(s) "State registrar" means that term as defined in section 2805 of the public health code, 1978 PA 368, MCL 333.2805.

(t) "Trade or commerce" means that term as defined in section 2 of the Michigan consumer protection act, 1971 PA 331, MCL 445.902.

(u) "Vital record" means that term as defined in section 2805 of the public health code, 1978 PA 368, MCL 333.2805.

History: 2004, Act 452, Eff. Mar. 1, 2005;—Am. 2006, Act 566, Eff. July 2, 2007.

445.65 Prohibited acts; violations; defense in civil action or criminal prosecution; burden of proof.

Sec. 5. (1) A person shall not do any of the following:

(a) With intent to defraud or violate the law, use or attempt to use the personal identifying information of another person to do either of the following:

(*i*) Obtain credit, goods, services, money, property, a vital record, a confidential telephone record, medical records or information, or employment.

(*ii*) Commit another unlawful act.

(b) By concealing, withholding, or misrepresenting the person's identity, use or attempt to use the personal identifying information of another person to do either of the following:

(*i*) Obtain credit, goods, services, money, property, a vital record, a confidential telephone record, medical records or information, or employment.

(*ii*) Commit another unlawful act.

(2) A person who violates subsection (1)(b)(*i*) may assert 1 or more of the following as a defense in a civil action or as an affirmative defense in a criminal prosecution, and has the burden of proof on that defense by a preponderance of the evidence:

(a) That the person gave a bona fide gift for or for the benefit or control of, or use or consumption by, the person whose personal identifying information was used.

(b) That the person acted in otherwise lawful pursuit or enforcement of a person's legal rights, including an investigation of a crime or an audit, collection, investigation, or transfer of a debt, child or spousal support

© Legislative Council, State of Michigan Courtesy of www.legislature.mi.gov

obligation, tax liability, claim, receivable, account, or interest in a receivable or account.

(c) That the action taken was authorized or required by state or federal law, rule, regulation, or court order or rule.

(d) That the person acted with the consent of the person whose personal identifying information was used, unless the person giving consent knows that the information will be used to commit an unlawful act.

History: 2004, Act 452, Eff. Mar. 1, 2005;—Am. 2006, Act 246, Imd. Eff. June 30, 2006.

445.65a Definitions; prohibited acts; obtaining confidential telephone records by law enforcement agency or telecommunication provider.

Sec. 5a. (1) As used in this act:

(a) "Confidential telephone record" means any of the following:

(*i*) Information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a service offered by a telecommunication provider subscribed to by any customer of that telecommunication provider.

(*ii*) Information that is made available to a telecommunication provider by a customer solely by virtue of the relationship between the telecommunication provider and the customer.

(*iii*) Information contained in any bill related to the product or service offered by a telecommunication provider and received by any customer of the telecommunication provider.

(b) "Covered specialized mobile radio service" means a commercial mobile radio service that offers real-time, 2-way switched voice or data service and is interconnected with the public switched network utilizing an in-network switching facility.

(c) "IP-enabled voice service" means an interconnected voice over internet protocol service that enables real-time, 2-way voice communications, requires a broadband connection from the user's location using internet protocol-compatible equipment, and permits users generally to receive calls that originate on the public switched telephone network and to terminate calls to the public switched telephone network.

(d) "Telecommunication provider" means all of the following:

(*i*) A provider as that term is defined in section 102 of the Michigan telecommunications act, 1991 PA 179, MCL 484.2102.

(*ii*) A provider of IP-enabled voice service.

(*iii*) A provider of any telecommunication service.

(e) "Telecommunication service" means all of the following:

(*i*) A service as that term is defined in section 102 of the Michigan telecommunications act, 1991 PA 179, MCL 484.2102.

(*ii*) Cellular telephone service.

(*iii*) Broadband personal communication service.

(*iv*) Covered specialized mobile radio.

(2) A person shall not do any of the following:

(a) Knowingly procure, attempt to procure, or solicit or conspire with another to procure a confidential telephone record of any resident of this state without the authorization of the customer to whom the record pertains or by fraudulent, deceptive, or false means.

(b) Knowingly sell or attempt to sell a confidential telephone record of any resident of this state without the authorization of the customer to whom the record pertains.

(c) Receive a confidential telephone record of any resident of this state knowing that the record has been obtained without the authorization of the customer to whom the record pertains or by fraudulent, deceptive, or false means.

(3) This section does not prohibit any action by a law enforcement agency, or any officer, employee, or agent of such agency, from obtaining confidential telephone records in connection with the performance of the official duties of the agency.

(4) This section does not prohibit a telecommunication provider from obtaining, using, disclosing, or permitting access to any confidential telephone record, either directly or indirectly, through its agents, subcontractors, affiliates, or representatives in the normal course of business. This section does not expand the obligations and duties of a telecommunication provider to protect confidential telephone records beyond those obligations and duties otherwise established by federal and state law.

History: Add. 2006, Act 246, Imd. Eff. June 30, 2006.

445.67 Additional prohibited acts.

Sec. 7. A person shall not do any of the following:

(a) Obtain or possess, or attempt to obtain or possess, personal identifying information of another person

© Legislative Council, State of Michigan Courtesy of www.legislature.mi.gov

with the intent to use that information to commit identity theft or another crime.

(b) Sell or transfer, or attempt to sell or transfer, personal identifying information of another person if the person knows or has reason to know that the specific intended recipient will use, attempt to use, or further transfer the information to another person for the purpose of committing identity theft or another crime.

(c) Falsify a police report of identity theft, or knowingly create, possess, or use a false police report of identity theft.

History: 2004, Act 452, Eff. Mar. 1, 2005.

445.69 Certain violations as felony; penalty; consecutive sentences; defense in civil action or criminal prosecution; burden of proof; exception.

Sec. 9. (1) Subject to subsection (6), a person who violates section 5 or 7 is guilty of a felony punishable by imprisonment for not more than 5 years or a fine of not more than $25,000.00, or both.

(2) Sections 5 and 7 apply whether an individual who is a victim or intended victim of a violation of 1 of those sections is alive or deceased at the time of the violation.

(3) This section does not prohibit a person from being charged with, convicted of, or sentenced for any other violation of law committed by that person using information obtained in violation of this section or any other violation of law committed by that person while violating or attempting to violate this section.

(4) The court may order that a term of imprisonment imposed under this section be served consecutively to any term of imprisonment imposed for a conviction of any other violation of law committed by that person using the information obtained in violation of this section or any other violation of law committed by that person while violating or attempting to violate this section.

(5) A person may assert as a defense in a civil action or as an affirmative defense in a criminal prosecution for a violation of section 5 or 7, and has the burden of proof on that defense by a preponderance of the evidence, that the person lawfully transferred, obtained, or attempted to obtain personal identifying information of another person for the purpose of detecting, preventing, or deterring identity theft or another crime or the funding of a criminal activity.

(6) Subsection (1) does not apply to a violation of a statute or rule administered by a regulatory board, commission, or officer acting under authority of this state or the United States that confers primary jurisdiction on that regulatory board, commission, or officer to authorize, prohibit, or regulate the transactions and conduct of that person, including, but not limited to, a state or federal statute or rule governing a financial institution and the insurance code of 1956, 1956 PA 218, MCL 500.100 to 500.8302, if the act is committed by a person subject to and regulated by that statute or rule, or by another person who has contracted with that person to use personal identifying information.

History: 2004, Act 452, Eff. Mar. 1, 2005.

445.71 Prohibited acts in conduct of trade or commerce; violation as misdemeanor.

Sec. 11. (1) A person shall not do any of the following in the conduct of trade or commerce:

(a) Deny credit or public utility service to or reduce the credit limit of a consumer solely because the consumer was a victim of identity theft, if the person had prior knowledge that the consumer was a victim of identity theft. A consumer is presumed to be a victim of identity theft for the purposes of this subdivision if he or she provides both of the following to the person:

(*i*) A copy of a police report evidencing the claim of the victim of identity theft.

(*ii*) Either a properly completed copy of a standardized affidavit of identity theft developed and made available by the federal trade commission pursuant to 15 USC 1681g or an affidavit of fact that is acceptable to the person for that purpose.

(b) Solicit to extend credit to a consumer who does not have an existing line of credit, or has not had or applied for a line of credit within the preceding year, through the use of an unsolicited check that includes personal identifying information other than the recipient's name, address, and a partial, encoded, or truncated personal identifying number. In addition to any other penalty or remedy under this act or the Michigan consumer protection act, 1976 PA 331, MCL 445.901 to 445.922, a credit card issuer, financial institution, or other lender that violates this subdivision, and not the consumer, is liable for the amount of the instrument if the instrument is used by an unauthorized user and for any fees assessed to the consumer if the instrument is dishonored.

(c) Solicit to extend credit to a consumer who does not have a current credit card, or has not had or applied for a credit card within the preceding year, through the use of an unsolicited credit card sent to the consumer. In addition to any other penalty or remedy under this act or the Michigan consumer protection act, 1976 PA 331, MCL 445.901 to 445.922, a credit card issuer, financial institution, or other lender that violates this subdivision, and not the consumer, is liable for any charges if the credit card is used by an unauthorized user

© Legislative Council, State of Michigan Courtesy of www.legislature.mi.gov

and for any interest or finance charges assessed to the consumer.

(d) Extend credit to a consumer without exercising reasonable procedures to verify the identity of that consumer. Compliance with regulations issued for depository institutions, and to be issued for other financial institutions, by the United States department of treasury under section 326 of the USA patriot act of 2001, 31 USC 5318, is considered compliance with this subdivision. This subdivision does not apply to a purchase of a credit obligation in an acquisition, merger, purchase of assets, or assumption of liabilities or any change to or review of an existing credit account.

(2) A person who knowingly or intentionally violates subsection (1) is guilty of a misdemeanor punishable by imprisonment for not more than 30 days or a fine of not more than $1,000.00, or both. This subsection does not affect the availability of any civil remedy for a violation of this act, the Michigan consumer protection act, 1976 PA 331, MCL 445.901 to 445.922, or any other state or federal law.

History: 2004, Act 452, Eff. Mar. 1, 2005.

445.72 Notice of security breach; requirements.

Sec. 12. (1) Unless the person or agency determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, 1 or more residents of this state, a person or agency that owns or licenses data that are included in a database that discovers a security breach, or receives notice of a security breach under subsection (2), shall provide a notice of the security breach to each resident of this state who meets 1 or more of the following:

(a) That resident's unencrypted and unredacted personal information was accessed and acquired by an unauthorized person.

(b) That resident's personal information was accessed and acquired in encrypted form by a person with unauthorized access to the encryption key.

(2) Unless the person or agency determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, 1 or more residents of this state, a person or agency that maintains a database that includes data that the person or agency does not own or license that discovers a breach of the security of the database shall provide a notice to the owner or licensor of the information of the security breach.

(3) In determining whether a security breach is not likely to cause substantial loss or injury to, or result in identity theft with respect to, 1 or more residents of this state under subsection (1) or (2), a person or agency shall act with the care an ordinarily prudent person or agency in like position would exercise under similar circumstances.

(4) A person or agency shall provide any notice required under this section without unreasonable delay. A person or agency may delay providing notice without violating this subsection if either of the following is met:

(a) A delay is necessary in order for the person or agency to take any measures necessary to determine the scope of the security breach and restore the reasonable integrity of the database. However, the agency or person shall provide the notice required under this subsection without unreasonable delay after the person or agency completes the measures necessary to determine the scope of the security breach and restore the reasonable integrity of the database.

(b) A law enforcement agency determines and advises the agency or person that providing a notice will impede a criminal or civil investigation or jeopardize homeland or national security. However, the agency or person shall provide the notice required under this section without unreasonable delay after the law enforcement agency determines that providing the notice will no longer impede the investigation or jeopardize homeland or national security.

(5) Except as provided in subsection (11), an agency or person shall provide any notice required under this section by providing 1 or more of the following to the recipient:

(a) Written notice sent to the recipient at the recipient's postal address in the records of the agency or person.

(b) Written notice sent electronically to the recipient if any of the following are met:

(*i*) The recipient has expressly consented to receive electronic notice.

(*ii*) The person or agency has an existing business relationship with the recipient that includes periodic electronic mail communications and based on those communications the person or agency reasonably believes that it has the recipient's current electronic mail address.

(*iii*) The person or agency conducts its business primarily through internet account transactions or on the internet.

(c) If not otherwise prohibited by state or federal law, notice given by telephone by an individual who represents the person or agency if all of the following are met:

© Legislative Council, State of Michigan Courtesy of www.legislature.mi.gov

(*i*) The notice is not given in whole or in part by use of a recorded message.

(*ii*) The recipient has expressly consented to receive notice by telephone, or if the recipient has not expressly consented to receive notice by telephone, the person or agency also provides notice under subdivision (a) or (b) if the notice by telephone does not result in a live conversation between the individual representing the person or agency and the recipient within 3 business days after the initial attempt to provide telephonic notice.

(d) Substitute notice, if the person or agency demonstrates that the cost of providing notice under subdivision (a), (b), or (c) will exceed $250,000.00 or that the person or agency has to provide notice to more than 500,000 residents of this state. A person or agency provides substitute notice under this subdivision by doing all of the following:

(*i*) If the person or agency has electronic mail addresses for any of the residents of this state who are entitled to receive the notice, providing electronic notice to those residents.

(*ii*) If the person or agency maintains a website, conspicuously posting the notice on that website.

(*iii*) Notifying major statewide media. A notification under this subparagraph shall include a telephone number or a website address that a person may use to obtain additional assistance and information.

(6) A notice under this section shall meet all of the following:

(a) For a notice provided under subsection (5)(a) or (b), be written in a clear and conspicuous manner and contain the content required under subdivisions (c) to (g).

(b) For a notice provided under subsection (5)(c), clearly communicate the content required under subdivisions (c) to (g) to the recipient of the telephone call.

(c) Describe the security breach in general terms.

(d) Describe the type of personal information that is the subject of the unauthorized access or use.

(e) If applicable, generally describe what the agency or person providing the notice has done to protect data from further security breaches.

(f) Include a telephone number where a notice recipient may obtain assistance or additional information.

(g) Remind notice recipients of the need to remain vigilant for incidents of fraud and identity theft.

(7) A person or agency may provide any notice required under this section pursuant to an agreement between that person or agency and another person or agency, if the notice provided pursuant to the agreement does not conflict with any provision of this section.

(8) Except as provided in this subsection, after a person or agency provides a notice under this section, the person or agency shall notify each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, as defined in 15 USC 1681a(p), of the security breach without unreasonable delay. A notification under this subsection shall include the number of notices that the person or agency provided to residents of this state and the timing of those notices. This subsection does not apply if either of the following is met:

(a) The person or agency is required under this section to provide notice of a security breach to 1,000 or fewer residents of this state.

(b) The person or agency is subject to title V of the Gramm-Leach-Bliley act, 15 USC 6801 to 6809.

(9) A financial institution that is subject to, and has notification procedures in place that are subject to examination by the financial institution's appropriate regulator for compliance with, the interagency guidance on response programs for unauthorized access to customer information and customer notice prescribed by the board of governors of the federal reserve system and the other federal bank and thrift regulatory agencies, or similar guidance prescribed and adopted by the national credit union administration, and its affiliates, is considered to be in compliance with this section.

(10) A person or agency that is subject to and complies with the health insurance portability and accountability act of 1996, Public Law 104-191, and with regulations promulgated under that act, 45 CFR parts 160 and 164, for the prevention of unauthorized access to customer information and customer notice is considered to be in compliance with this section.

(11) A public utility that sends monthly billing or account statements to the postal address of its customers may provide notice of a security breach to its customers in the manner described in subsection (5), or alternatively by providing all of the following:

(a) As applicable, notice as described in subsection (5)(b).

(b) Notification to the media reasonably calculated to inform the customers of the public utility of the security breach.

(c) Conspicuous posting of the notice of the security breach on the website of the public utility.

(d) Written notice sent in conjunction with the monthly billing or account statement to the customer at the customer's postal address in the records of the public utility.

(12) A person that provides notice of a security breach in the manner described in this section when a

© Legislative Council, State of Michigan Courtesy of www.legislature.mi.gov

security breach has not occurred, with the intent to defraud, is guilty of a misdemeanor punishable by imprisonment for not more than 30 days or a fine of not more than $250.00 for each violation, or both.

(13) Subject to subsection (14), a person that knowingly fails to provide any notice of a security breach required under this section may be ordered to pay a civil fine of not more than $250.00 for each failure to provide notice. The attorney general or a prosecuting attorney may bring an action to recover a civil fine under this section.

(14) The aggregate liability of a person for civil fines under subsection (13) for multiple violations of subsection (13) that arise from the same security breach shall not exceed $750,000.00.

(15) Subsections (12) and (13) do not affect the availability of any civil remedy for a violation of state or federal law.

(16) This section applies to the discovery or notification of a breach of the security of a database that occurs on or after the effective date of the amendatory act that added this section.

(17) This section does not apply to the access or acquisition by a person or agency of federal, state, or local government records or documents lawfully made available to the general public.

(18) This section deals with subject matter that is of statewide concern, and any charter, ordinance, resolution, regulation, rule, or other action by a municipal corporation or other political subdivision of this state to regulate, directly or indirectly, any matter expressly set forth in this section is preempted.

History: Add. 2006, Act 566, Eff. July 2, 2007.

445.72a Destruction of data containing personal information required; violation as misdemeanor; fine; compliance; "destroy" defined.

Sec. 12a. (1) Subject to subsection (3), a person or agency that maintains a database that includes personal information regarding multiple individuals shall destroy any data that contain personal information concerning an individual when that data is removed from the database and the person or agency is not retaining the data elsewhere for another purpose not prohibited by state or federal law. This subsection does not prohibit a person or agency from retaining data that contain personal information for purposes of an investigation, audit, or internal review.

(2) A person who knowingly violates this section is guilty of a misdemeanor punishable by a fine of not more than $250.00 for each violation. This subsection does not affect the availability of any civil remedy for a violation of state or federal law.

(3) A person or agency is considered to be in compliance with this section if the person or agency is subject to federal law concerning the disposal of records containing personal identifying information and the person or agency is in compliance with that federal law.

(4) As used in this section, "destroy" means to destroy or arrange for the destruction of data by shredding, erasing, or otherwise modifying the data so that they cannot be read, deciphered, or reconstructed through generally available means.

History: Add. 2006, Act 566, Eff. July 2, 2007.

445.72b Misrepresentation by advertisement or solicitation prohibited; violation as misdemeanor; penalty.

Sec. 12b. (1) A person shall not distribute an advertisement or make any other solicitation that misrepresents to the recipient that a security breach has occurred that may affect the recipient.

(2) A person shall not distribute an advertisement or make any other solicitation that is substantially similar to a notice required under section 12(5) or by federal law, if the form of that notice is prescribed by state or federal law, rule, or regulation.

(3) A person who knowingly or intentionally violates this section is guilty of a misdemeanor punishable by imprisonment for not more than 30 days or a fine of not more than $1,000.00 for each violation, or both. This subsection does not affect the availability of any civil remedy for a violation of this section or any other state or federal law.

History: Add. 2006, Act 566, Eff. July 2, 2007.

445.73 Verification of information; use of vital record.

Sec. 13. (1) A law enforcement agency or victim of identity theft may verify information from a vital record from a local registrar or the state registrar in the manner described in section 2881(2) of the public health code, 1978 PA 368, MCL 333.2881.

(2) A state registrar or local registrar that verifies information from a vital record under section 2881(2) of the public health code, 1978 PA 368, MCL 333.2881, for a law enforcement agency investigating identity theft may provide that law enforcement agency with all of the following information about any previous

© Legislative Council, State of Michigan Courtesy of www.legislature.mi.gov

requests concerning that public record that is available to the registrar:

(a) Whether or not a certified copy or copies of the record were requested.

(b) The date or dates a copy or copies of the record were issued.

(c) The name of each applicant who requested the record.

(d) The address, e-mail address, telephone number, and other identifying information of each applicant who requested the record.

(e) Payment information regarding each request.

(3) A state registrar or local registrar that verifies information from a vital record under section 2881(2) of the public health code, 1978 PA 368, MCL 333.2881, for an individual who provides proof that he or she is a victim of identity theft may provide that individual with all of the following information about any previous requests concerning that public record that is available to the registrar:

(a) Whether or not a certified copy or copies of the record were requested.

(b) The date or dates a copy or copies of the record were issued.

(4) For purposes of subsection (3), it is sufficient proof that an individual is a victim of identity theft for a state registrar or local registrar to provide the information described in that subsection if he or she provides the registrar with a copy of a police report evidencing the claim that he or she is a victim of identity theft; and, if available, an affidavit of identity theft, in a form developed by the state registrar in cooperation with the attorney general for purposes of this subsection.

(5) A law enforcement agency may request an administrative use copy of a vital record from the state registrar in the manner described in section 2891 of the public health code, 1978 PA 368, MCL 333.2891.

(6) A law enforcement agency may request an administrative use copy of a vital record from a local registrar in the manner described in section 2891 of the public health code, 1978 PA 368, MCL 333.2891, if the request for the administrative use copy is in writing and contains both of the following:

(a) A statement that the law enforcement agency requires information from a vital record beyond the information the local registrar may verify under subsections (1) and (2).

(b) The agreement of the law enforcement agency that it will maintain the administrative use copy of the vital record in a secure location and will destroy the copy by confidential means when it no longer needs the copy.

History: 2004, Act 452, Eff. Mar. 1, 2005.

445.75 Repeal of MCL 750.285.

Sec. 15. Section 285 of the Michigan penal code, 1931 PA 328, MCL 750.285, is repealed.

History: 2004, Act 452, Eff. Mar. 1, 2005.

445.77 Effective date.

Sec. 17. This act takes effect March 1, 2005.

History: 2004, Act 452, Eff. Mar. 1, 2005.

© Legislative Council, State of Michigan Courtesy of www.legislature.mi.gov